ABSTRACT OF THE DISCLOSURE

The present invention provides a parallelizable integrity-aware encryption technique. In at least one embodiment of the invention, a parallelizable integrity-aware encryption method comprises whitening at least one message block with a first mask value, encrypting the whitened at least one message block using a block cipher and a first key, and whitening the encrypted at least one message block with a second mask value to generate at least one corresponding output ciphertext block. In another embodiment of the invention, a parallelizable integrity-aware encryption method comprises applying a XOR function to all blocks of a message to compute a XOR-sum, applying a first mask value to the XOR-sum; encrypting the masked XOR-sum using a block cipher and a first key, and applying a second mask value to the encrypted XOR-sum to generate an integrity tag.